BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月１２日

出願番号
Application Number: 特願２００４－０３５４８１

[ST. 10/C]: [ＪＰ２００４－０３５４８１]

出願人
Applicant(s): 富士ゼロックス株式会社

２００４年　３月２４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０２４３０５

【書類名】　特許願
【整理番号】　FE04-00132
【提出日】　平成16年 2月12日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/46　100
【発明者】
　【住所又は居所】　東京都港区赤坂二丁目１７番２２号　富士ゼロックス株式会社内
　【氏名】　吉田　武央
【特許出願人】
　【識別番号】　000005496
　【氏名又は名称】　富士ゼロックス株式会社
【代理人】
　【識別番号】　110000154
　【氏名又は名称】　特許業務法人はるか国際特許事務所
　【代表者】　金山　敏彦
　【電話番号】　03-5367-2790
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 59162
　【出願日】　平成15年 3月 5日
【手数料の表示】
　【予納台帳番号】　185835
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0301849

【書類名】特許請求の範囲
【請求項１】
クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムであって、
前記認証用サーバは、
前記接続サーバにおいて利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、
前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得する手段と、
前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、
を含み、
前記クライアント装置は、
前記認証用サーバに対し、前記第２接続認証情報を、ユーザを特定する情報として、接続要求とともに送信する手段と、
前記認証用サーバから前記接続サーバのアドレスを受信する手段と、
前記受信した接続サーバのアドレスに対し、第１接続認証情報を送信する手段と、
を含み、
前記接続サーバは、
前記認証用サーバから受信したクライアントアドレスからの接続を受け付ける手段と
前記クライアントアドレスから送信される、第１接続認証情報を用いて認証処理を行う手段と
を含む、
ことを特徴とするネットワーク接続システム。
【請求項２】
請求項１に記載のネットワーク接続システムにおいて、
前記第２接続認証情報は、前記第１接続認証情報のメッセージダイジェストである
ことを特徴とするネットワーク接続システム。
【請求項３】
クライアント装置と、接続サーバと、に接続される認証用サーバであって、
前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、
前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、
前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、
を含むことを特徴とする認証用サーバ。
【請求項４】
認証用サーバと、接続サーバと、に接続されるクライアント装置であって、
前記認証用サーバに対して、前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報とともに接続要求を送信する接続要求手段と、
前記認証用サーバから前記接続サーバのアドレスを受信して、前記受信した接続サーバのアドレスに対し、第１接続認証情報を送信する手段と、
を含む

ことを特徴とするクライアント装置。
【請求項５】
認証用サーバと、クライアント装置と、に接続される接続サーバであって、
前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手段と、
当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手段と、
を含む
ことを特徴とする接続サーバ。
【請求項６】
クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムであって、
前記認証用サーバは、
第１の暗号化方法で暗号化された第１暗号化ユーザ名と第１暗号化パスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、
前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、第１暗号化ユーザ名及び第１暗号化パスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、
前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、
を含み、
前記クライアント装置は、
前記認証用サーバに対して、第１の暗号化方法で暗号化された第１暗号化ユーザ名及び第１暗号化パスワードとともに、接続要求を送信する手段と、
前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化して生成した、第２暗号化ユーザ名及び第２暗号化パスワードを、前記受信したネットワークアドレスに対して送信する手段と、
を含み、
前記接続サーバ側で、当該第２暗号化ユーザ名及び第２暗号化パスワードを用いた認証が行われる
ことを特徴とするネットワーク接続システム。
【請求項７】
クライアント装置と、接続サーバと、に接続される認証用サーバであって、
所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、
前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、前記暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、
前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、
を含むことを特徴とする認証用サーバ。

【請求項８】
認証用サーバと、接続サーバと、に接続されるクライアント装置であって、
前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手段と、
前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化し、当該第２の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手段と、
を含む
ことを特徴とするクライアント装置。
【請求項９】
請求項８に記載のクライアント装置であって、
当該クライアント装置に固有の固有情報と、ユーザ名及びパスワードの少なくともいずれか一方とを関連付ける情報として、前記接続サーバから予め提供されているローカル認証用情報を保持する手段と、
ユーザからユーザ名及びパスワードの入力を受け付けると、前記固有情報を生成し、前記ローカル認証用情報を参照して、当該受け付けたユーザ名及びパスワードの少なくともいずれか一方が、前記生成した固有情報に関連付けられているか否かを調べることにより、当該ユーザを認証するローカル認証手段と、
を含み、
前記接続要求手段は、前記ローカル認証手段により、ユーザの認証が行われた場合にのみ、前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する
ことを特徴とするクライアント装置。
【請求項１０】
クライアント装置と、認証用サーバと、に接続される接続サーバであって、
前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信する
ことを特徴とする接続サーバ。
【請求項１１】
クライアント装置と、前記クライアント装置に対して接続先を案内する情報を提供する認証用サーバと、接続サーバとを含むネットワーク接続システムであって、
前記クライアント装置は、当該クライアント装置に固有の第１認証情報を演算して、予め前記接続サーバに登録するとともに、前記接続サーバから、当該第１認証情報と、所定の第２認証情報とを関連付けるローカル認証用情報を取得して保持しており、
ユーザから前記接続サーバに対する接続要求の指示があったときに、前記第２認証情報の入力を受けるとともに、クライアント装置に固有の第１認証情報を改めて演算し、前記保持しているローカル認証用情報を用いて、入力を受けた第２認証用情報と、改めて演算した第１認証用情報との関連づけを調べ、関連付けられていると判断される場合に、前記第２認証用情報を第１の暗号化方法で暗号化し、前記認証用サーバに対して当該第１の暗号化方法で暗号化した第２認証用情報を送信し、
前記接続サーバのネットワークアドレスを、接続先を案内する情報として前記認証用サーバから受信して、当該接続サーバのネットワークアドレスに対して、第２の暗号化方法で暗号化した第２認証用情報を送信して、前記接続サーバとの通信を開始することを特徴とするネットワーク接続システム。
【請求項１２】
クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法であって、

前記認証用サーバは、前記接続サーバにおいて利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持しており、

前記クライアント装置が、前記認証用サーバに対し、前記第２接続認証情報を、ユーザを特定する情報として、接続要求とともに送信し、

前記認証用サーバが、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得し、前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出し、

前記クライアント装置が、前記認証用サーバから前記接続サーバのアドレスを受信し、当該受信した接続サーバのアドレスに対し、第１接続認証情報を送信し、

前記接続サーバが、前記認証用サーバから受信したクライアントアドレスからの接続を受け付けて、当該クライアントアドレスを利用する前記クライアントアドレスから送信される、第１接続認証情報を用いて認証処理を行う、

ことを特徴とする接続方法。

【請求項１３】

クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法であって、

前記認証サーバは、第１の暗号化方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持しており、

前記クライアント装置が、前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信し、

前記認証サーバが、当該クライアント装置から接続要求を受信して、当該クライアント装置のユーザを特定する情報として、第１の暗号化方法で暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得し、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、

前記接続サーバが、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信し、

前記認証用サーバが、前記接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出し、

前記クライアント装置が、前記認証用サーバから受信した、前記接続サーバのネットワークアドレスに対して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化し、当該第２の暗号化方法で暗号化したユーザ名及びパスワードを送信し、

前記接続サーバが、当該クライアント装置から受信した、第２の暗号化方法で暗号化されたユーザ名及びパスワードを用いてユーザの認証を行う

ことを特徴とする接続方法。

【請求項１４】

クライアント装置と、接続サーバと、に接続される認証用サーバに、

前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する手順と、

前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワ

ークアドレスをクライアントアドレスとして取得する手順と、
前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手順と、
を実行させることを特徴とするプログラム。
【請求項１５】
認証用サーバと、接続サーバと、に接続されるクライアント装置に、
前記認証用サーバに対して、前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報とともに接続要求を送信する手順と、
前記認証用サーバから前記接続サーバのアドレスを受信して、前記受信した接続サーバのアドレスに対し、第１接続認証情報を送信する手順と、
を実行させることを特徴とするプログラム。
【請求項１６】
認証用サーバと、クライアント装置と、に接続される接続サーバに、
前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手順と、
当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手順と、
を実行させることを特徴とするプログラム。
【請求項１７】
クライアント装置と、接続サーバと、に接続される認証用サーバに、
所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持手段に保持する手順と、
前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手順と、
前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手順と、
を実行させることを特徴とするプログラム。
【請求項１８】
認証用サーバと、接続サーバと、に接続されるクライアント装置に、
前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手順と、
前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化し、当該第２の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手順と、
を実行させることを特徴とするクライアント装置用プログラム。
【請求項１９】
クライアント装置と、前記クライアント装置との間で暗号化通信を行う認証用サーバとに接続される接続サーバに、
前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信する手順、

を実行させることを特徴とする接続サーバ用プログラム。

【書類名】明細書
【発明の名称】ネットワーク接続システム
【技術分野】
【０００１】
本発明は、ローカルネットワーク等にリモートからの接続を可能とするネットワーク接続システムに関する。
【背景技術】
【０００２】
近年では、インターネット接続環境の普及と相俟って、個々人のワーキングスタイルが多様化しつつある。例えば、企業に属しながら自宅で仕事を行う、いわゆる在宅型のワーキングスタイルも受け入れられ易くなってきている。これは、企業内のローカルネットワークに対してインターネットや公衆電話回線網等、異なるユーザが共用するネットワークを経由して、自宅等、遠隔地からアクセスする、いわゆるリモートアクセスサービス（ＲＡＳ）技術の開発が進展してきたからである。
【０００３】
こうしたリモートアクセスサービスでは、企業内で利用される情報が、外部から自由に参照されることを防止するため、予めローカルネットワークに登録されたユーザ名と、パスワードとによってローカルネットワーク側で認証を行うとともに、遠隔地とアクセス先であるローカルネットワークとの間のネットワーク（途中のネットワーク）上での認証後のトラフィックを暗号化しているのが普通である。
【０００４】
なお、複数のサーバのユーザ認証情報を保持していない端末からも、それらをアクセスでき、各サーバの課金をまとめて管理するシステムを提供する目的で、中間サーバから各端末が、接続先となるサーバへの接続に必要な情報を取得する技術が特許文献１に開示されている。
【特許文献１】特開平０８－２３５１１４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記従来のリモートアクセスサービスでは、認証後のトラフィックは暗号化されるものの、ユーザ名等の認証用の情報はそのまま流通する。従って、ユーザ名が途中のネットワークで不正に取得された場合、ローカルネットワーク側に対して、当該不正に取得したユーザ名を送出し、パスワードとしてランダムにアタックをしかけるタイプの不正アクセスが可能になる。
【０００６】
本発明は上記実情に鑑みて為されたもので、リモートアクセスにおけるセキュリティを向上できるネットワーク接続システムを提供することを、その目的の一つとする。
【課題を解決するための手段】
【０００７】
上記従来例の問題点を解決するための本発明は、クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムであって、前記認証用サーバは、前記接続サーバにおいて利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、を含み、前記クライアント装置は、前記認証用サーバに対し、前記第２接続認

証情報を、ユーザを特定する情報として、接続要求とともに送信する手段と、前記認証用サーバから前記接続サーバのアドレスを受信する手段と、前記受信した接続サーバのアドレスに対し、第１接続認証情報を送信する手段と、を含み、前記接続サーバは、前記認証用サーバから受信したクライアントアドレスからの接続を受け付ける手段と前記クライアントアドレスから送信される、第１接続認証情報を用いて認証処理を行う手段とを含む、ことを特徴としている。

【０００８】

またここで、前記第２接続認証情報は、前記第１接続認証情報のメッセージダイジェストであることとしてもよい。

【０００９】

また上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバであって、前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手段と、を含むことを特徴としている。

【００１０】

また、上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置であって、前記認証用サーバに対して、前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報とともに接続要求を送信する接続要求手段と、前記認証用サーバから前記接続サーバのアドレスを受信して、第１接続認証情報を、前記受信した接続サーバのアドレスに対して送信する手段と、を含むことを特徴としている。

【００１１】

また、上記従来例の問題点を解決するための本発明は、認証用サーバと、クライアント装置と、に接続される接続サーバであって、前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手段と、当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手段と、を含むことを特徴としている。

【００１２】

また、本発明のある態様に係るクライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムでは、前記認証用サーバは、第１の暗号化方法で暗号化された第１暗号化ユーザ名と第１暗号化パスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、第１暗号化ユーザ名及び第１暗号化パスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、を含み、前記クライアント装置は、前記認証用サーバに対して、第１の暗号化方法で暗号化された第１暗号化ユーザ名及び第１暗号化パスワードとともに、接続要求を送信する手段と、前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化し

て生成した、第２暗号化ユーザ名及び第２暗号化パスワードを、前記受信したネットワークアドレスに対して送信する手段と、を含み、前記接続サーバ側で、当該第２暗号化ユーザ名及び第２暗号化パスワードを用いた認証が行われることを特徴としている。

【００１３】

このようにしたので、クライアント装置のユーザは、認証用サーバにおいて認証を受けるまでは、接続サーバのネットワークアドレスを知ることもできない。さらに、認証サーバ及び接続サーバに対して送出されるユーザ名等は、それぞれ第１、第２の暗号化方法、例えばハッシュ関数によって暗号化されたり、所与のランダム情報をユーザ名等をキーとして暗号化するといった方法で暗号化されているため、ユーザ名等が漏えいすることが防止され、セキュリティを向上させることができる。なお、第１、第２の暗号化方法は互いに異なる方法であってもよいし、同じ方法であってもよい。

【００１４】

上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバであって、所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持する保持手段と、前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、前記暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手段と、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手段と、を含むことを特徴としている。

【００１５】

また上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置であって、前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手段と、前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化し、当該第２の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手段と、を含むことを特徴としている。

【００１６】

ここで、このクライアント装置は、クライアント装置に固有の固有情報と、ユーザ名及びパスワードの少なくともいずれか一方とを関連付ける情報として、前記接続サーバから予め提供されているローカル認証用情報を保持する手段と、ユーザからユーザ名及びパスワードの入力を受け付けると、前記固有情報を生成し、前記ローカル認証用情報を参照して、当該受け付けたユーザ名及びパスワードの少なくともいずれか一方が、前記生成した固有情報に関連付けられているか否かを調べることにより、当該ユーザを認証するローカル認証手段と、を含み、前記接続要求手段は、前記ローカル認証手段により、ユーザの認証が行われた場合にのみ、前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信することとしてもよい。

【００１７】

また、上記従来例の問題点を解決するための本発明は、クライアント装置と、認証用サーバと、に接続される接続サーバであって、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信することを特徴としている。

【００１８】

さらに、上記従来例の問題点を解決するための本発明は、クライアント装置と、前記クライアント装置に対して接続先を案内する情報を提供する認証用サーバと、接続サーバと

を含むネットワーク接続システムであって、前記クライアント装置は、当該クライアント装置に固有の第１認証情報を演算して、予め前記接続サーバに登録するとともに、前記接続サーバから、当該第１認証情報と、所定の第２認証情報とを関連付けるローカル認証用情報を取得して保持しており、ユーザから前記接続サーバに対する接続要求の指示があったときに、前記第２認証情報の入力を受けるとともに、クライアント装置に固有の第１認証情報を改めて演算し、前記保持しているローカル認証用情報を用いて、入力を受けた第２認証用情報と、改めて演算した第１認証用情報との関連づけを調べ、関連付けられていると判断される場合に、前記第２認証用情報を第１の暗号化方法で暗号化し、前記認証用サーバに対して当該第１の暗号化方法で暗号化した第２認証用情報を送信し、前記接続サーバのネットワークアドレスを、接続先を案内する情報として前記認証用サーバから受信して、当該接続サーバのネットワークアドレスに対して、第２の暗号化方法で暗号化した第２認証用情報を送信して、前記接続サーバとの通信を開始することとしている。

【００１９】

また、本発明の一態様に係る、クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法は、前記認証用サーバが、前記接続サーバにおいて利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持しており、前記クライアント装置が、前記認証用サーバに対し、前記第２接続認証情報を、ユーザを特定する情報として、接続要求とともに送信し、前記認証用サーバが、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスを、クライアントアドレスとして取得し、前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報により特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出し、前記クライアント装置が、前記認証用サーバから前記接続サーバのアドレスを受信し、当該受信した接続サーバのアドレスに対し、第１接続認証情報を送信し、前記接続サーバが、前記認証用サーバから受信したクライアントアドレスからの接続を受け付けて、当該クライアントアドレスを利用する前記クライアントアドレスから送信される、第１接続認証情報を用いて認証処理を行うものである。

【００２０】

さらに、本発明の一態様に係る、ネットワークへの接続方法は、クライアント装置と、認証用サーバと、接続サーバとを含むネットワーク接続システムを用いた接続方法であって、前記認証サーバは、第１の暗号化方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持しており、前記クライアント装置が、前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信し、前記認証サーバが、当該クライアント装置から接続要求を受信して、当該クライアント装置のユーザを特定する情報として、第１の暗号化方法で暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得し、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、前記接続サーバが、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信し、前記認証用サーバが、前記接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出し、前記クライアント装置が、前記認証用サーバから受信した、前記接続サーバのネットワークアドレスに対して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化し、当該第２の暗号化方法で暗号化

したユーザ名及びパスワードを送信し、前記接続サーバが、当該クライアント装置から受信した、第２の暗号化方法で暗号化されたユーザ名及びパスワードを用いてユーザの認証を行うことを特徴としている。

【００２１】

また、上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバにより実行されるプログラムであって、前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報を、当該接続サーバを特定する情報に関連づけて保持する手順と、前記クライアント装置から接続要求を受信したときに、該クライアント装置からユーザを特定する情報を取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手順と、前記ユーザを特定する情報が、前記第２接続認証情報に適合する場合に、当該第２接続認証情報に関連づけられた情報によって特定される接続サーバに対して、前記取得したクライアントアドレスを送信するとともに、当該接続サーバのネットワークアドレスを、前記接続要求元のクライアント装置に対して送出する手順と、を前記認証用サーバに実行させることを特徴としている。

【００２２】

また、上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置により実行されるプログラムであって、前記認証用サーバに対して、前記接続サーバで利用される第１接続認証情報、に基づいて作成される第２接続認証情報とともに接続要求を送信する手順と、前記認証用サーバから前記接続サーバのアドレスを受信して、前記受信した接続サーバのアドレスに対し、第１接続認証情報を送信する手順と、を前記クライアント装置に実行させることを特徴としている。

【００２３】

さらに、上記従来例の問題点を解決するための本発明は、認証用サーバと、クライアント装置と、に接続される接続サーバによって実行されるプログラムであって、前記認証用サーバから前記クライアント装置のクライアントアドレスを受信して、該クライアントアドレスからの接続を受入可能に制御する手順と、当該受入可能となったクライアントアドレスを利用するクライアント装置から認証用情報を受信し、当該認証用情報を用いた認証を行う手順と、を前記接続サーバに実行させることを特徴としている。

【００２４】

また、上記従来例の問題点を解決するための本発明は、クライアント装置と、接続サーバと、に接続される認証用サーバに、所定の方法で暗号化されたユーザ名とパスワードとを、前記接続サーバのネットワークアドレスに関連付けて保持手段に保持する手順と、前記クライアント装置から接続要求を受信したときに、当該クライアント装置のユーザを特定する情報として、暗号化されたユーザ名及びパスワードを取得するとともに、当該クライアント装置が現在利用しているネットワークアドレスをクライアントアドレスとして取得する手順と、前記ユーザを特定する情報が、前記保持手段に保持されている場合に、当該ユーザを特定する情報に関連付けられた接続サーバのネットワークアドレスに対して、前記取得したクライアントアドレスを送信し、当該接続サーバから接続待機状態に移行した旨を表す情報を受信して、当該接続サーバのネットワークアドレスを、前記接続要求を行ったクライアント装置に対して送出する手順と、を実行させることを特徴としている。

【００２５】

さらに、上記従来例の問題点を解決するための本発明は、認証用サーバと、接続サーバと、に接続されるクライアント装置に、前記認証用サーバに対して、第１の暗号化方法で暗号化されたユーザ名及びパスワードとともに、接続要求を送信する接続要求手順と、前記認証用サーバから前記接続サーバのネットワークアドレスを受信して、ユーザから入力されたユーザ名と、パスワードとを第２の暗号化方法で暗号化し、当該第２の暗号化方法で暗号化したユーザ名及びパスワードを、前記受信したネットワークアドレスに対して送信する手順と、を実行させることを特徴としている。

【００２６】

さらに上記従来例の問題点を解決するための本発明は、クライアント装置と、前記クライアント装置との間で暗号化通信を行う認証用サーバとに接続される接続サーバに、前記認証用サーバから、接続しようとするクライアント装置のアドレスであるクライアントアドレスの通知を受けて、当該クライアントアドレスからの通信を、予め定められた一定の期間だけ受入可能に設定し、接続待機状態に移行した旨を表す情報を当該認証用サーバに対して送信する手順、を実行させることを特徴としている。

【発明を実施するための最良の形態】

【００２７】

本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るネットワーク接続システムは、図１に示すように、ローカルネットワーク１と、公衆ネットワーク２と、この公衆ネットワーク２に接続されたクライアント装置３と、認証サーバ４とを含んで構成されている。ローカルネットワーク１は、接続サーバ１１を介して公衆ネットワーク２に接続されている。公衆ネットワーク２は、インターネットや公衆電話回線網などからなるネットワークシステムである。なお図１では認証サーバ４は一つしか図示していないが、認証サーバ４は複数あっても構わない。

【００２８】

クライアント装置３は、一般的なパーソナルコンピュータであり、図１に示したように制御部３１と、記憶部３２と、通信制御部３３と、表示部３４と、操作部３５とを含む。制御部３１は、記憶部３２に格納されているプログラム（クライアント装置用プログラム）に従って動作している。この制御部３１は、ローカルネットワーク１へのＲＡＳ接続処理を実行する。このＲＡＳ接続処理の具体的内容については後に詳しく述べる。記憶部３２は、プログラムなどを格納する、コンピュータ読み取り可能な記憶媒体である。この記憶部３２は、また、制御部３１のワークメモリとしても動作する。

【００２９】

通信制御部３３は、制御部３１から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対して情報を送信する。また、この通信制御部３３は、ネットワークを介して到来する情報を受信して制御部３１に出力する。表示部３４は、制御部３１から入力される指示に従って情報を表示するディスプレイ装置などである。操作部３５は、キーボードやマウスなどであり、ユーザの指示操作の内容を制御部３１に対して出力する。

【００３０】

認証サーバ４は、一般的なサーバコンピュータであり、制御部４１と、記憶部４２と、通信制御部４３とを含んで構成される。制御部４１は、記憶部４２に格納されているプログラム（認証サーバ用プログラム）に従って動作し、認証処理を行う。この認証処理の具体的内容については後に詳しく述べる。

【００３１】

記憶部４２は、プログラムなどを格納する、コンピュータ読み取り可能な記憶媒体である。この記憶部４２はまた、制御部４１のワークメモリとしても動作する。通信制御部４３は、制御部４１から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対して情報を送信する。また、この通信制御部４３は、ネットワークを介して到来する情報を受信して制御部４１に出力する。

【００３２】

また、ローカルネットワーク１の接続サーバ１１もまた、一般的なサーバコンピュータであってよく、制御部１５と、記憶部１６と、第１通信制御部１７と、第２通信制御部１８とを含んで構成される。制御部１５は、記憶部１６に格納されているプログラム（接続サーバ用プログラム）に従って動作し、認証処理と接続処理等を行う。これらの認証処理や接続処理の具体的内容については後に詳しく述べる。

【００３３】

記憶部１６は、プログラムなどを格納する、コンピュータ読み取り可能な記憶媒体である。この記憶部１６はまた、制御部１５のワークメモリとしても動作する。第１通信制御

部１７は、制御部１５から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対し、公衆ネットワーク２を介して情報を送信する。また、この第１通信制御部１７は、公衆ネットワーク２を介して到来する情報を受信して制御部１５に出力する。第２通信制御部１８は、制御部１５から入力される指示に従って、当該指示に含まれるネットワークアドレスで特定される宛先に対し、ローカルネットワーク１を介して情報を送信する。また、この第２通信制御部１８は、ローカルネットワーク１を介して到来する情報を受信して制御部１５に出力する。

【００３４】

この接続サーバ１１の制御部１５は、後に説明する方法で認証したクライアント装置３から、第１通信制御部１７を介して受信する、データの要求などを第２通信制御部１８を介してローカルネットワーク１側に伝達する。また、ローカルネットワーク１側からクライアント装置３へ送信すべきデータ等を第２通信制御部１８を介して受け入れ、第１通信制御部１７を介して送信する。

【００３５】

[セットアップ]

ここで、クライアント装置３と、認証サーバ４と、接続サーバ１１との間で行われる認証処理について説明する。まず、クライアント装置３が、接続サーバ１１を介してＲＡＳ接続可能となるまでのセットアップの手順を述べる。なお、以下の説明において、クライアント装置３と認証サーバ４との間の通信は、広く知られたＳＳＬ（Secure Socket Layer）などの方法で暗号化されていることとしてもよい。

【００３６】

本実施の形態において特徴的なことの一つは、クライアント装置３に対してＲＡＳ接続のための専用のアプリケーションソフトウエアがインストールされることである。この専用アプリケーションソフトウエアは、暗号化された認証サーバ４のネットワークアドレスを保持しており、また、当該暗号化された認証サーバ４のネットワークアドレスを復号する手順をクライアント装置３に実行させ、クライアント装置３は、この専用アプリケーションソフトウエアによらなければ、認証サーバ４に対するアクセスが事実上できないようになっている。

【００３７】

次に、この専用アプリケーションソフトウエアのセットアップ手順を説明する。クライアント装置３に、この専用アプリケーションソフトウエアがインストールされると、クライアント装置３は、当該クライアント装置に固有の第１認証情報として、クライアント装置３を構成するハードディスクのシリアル番号など、ハードウエア関係情報や、オペレーティングシステムのバージョンなどソフトウエア環境に関係する情報といったクライアント装置３ごとに一般に異なる情報に基づいて、クライアント装置３の固有情報を演算する。

【００３８】

ユーザは、この固有情報と、ユーザ名、パスワードといった情報を接続サーバ１１の管理者に伝達する。この伝達方法は、例えば暗号化した電子メールであってもよいし、磁気ディスク等を利用した伝達手段によってもよい。接続サーバ１１の管理者は、これら固有情報、ユーザ名、パスワードを接続サーバ１１に登録する。接続サーバ１１は、この登録を受けて、当該ユーザを認証する認証サーバ４を選定し、当該選定した認証サーバ４のネットワークアドレスを暗号化して暗号化アドレスを生成し、また、所定の情報（任意の文字列でもよいし、ＲＡＳ接続の有効期限などといった意味ある情報でもよい）を、固有情報をキーとして暗号化した第１情報と、当該所定の情報を、ユーザ名をキーとして暗号化した第２情報とを生成する。そして接続サーバ１１は、これら暗号化アドレスと、第１情報と、第２情報とを含む情報を、定義情報として出力する。これら第１情報と第２情報とが、第１認証情報と第２認証情報とを関連付けるローカル認証用情報に相当する。またこの定義情報には、パスワードを、後に説明する第１の暗号化方法で暗号化した、暗号化パスワードの少なくとも一部を含んでもよい。

【００３９】
この定義情報は、クライアント装置３のユーザへの電子メール等、任意の方法でクライアント装置３側に提供され、クライアント装置３の記憶部３２に格納される。クライアント装置３は、専用アプリケーションソフトウエアに従って、この定義情報を利用して固有情報が誤りなく登録されたか否かを調べる。具体的には、固有情報を演算して生成するとともにユーザに対してユーザ名を入力させ、第１情報を生成した固有情報で復号し、第２情報を当該入力されたユーザ名で復号する。そしてこれらの復号結果（正しく復号されればいずれも上記所定の情報となる）が互いに一致するか否かを調べ、一致する場合に、固有情報が誤りなく登録されたと判断する。
【００４０】
一方、接続サーバ１１は、第１通信制御部１７側に割り当てられているネットワークアドレス（公衆ネットワーク側のアドレス）と、クライアント装置３のユーザ名及びパスワードを第１の暗号化方法で暗号化したものとを認証サーバ４に対して送信する。ここでのユーザ名及びパスワードの暗号化方法（第１の暗号化方法）は、復号可能なものでなくてもよく、ユーザ名及びパスワードのそれぞれについてのＭＤ５等のハッシュ値を用いるなど、メッセージダイジェストを利用してもよい。認証サーバ４は、図２に示すように、当該接続サーバ１から受信したネットワークアドレスと、第１の暗号化方法で暗号化されたユーザ名及びパスワードを関連付けて、保持手段としての記憶部４２に格納する。こうして一連のセットアップが完了する。
【００４１】
［認証処理］
次に、実際に接続要求が為された場合の認証処理について図３及び図４を参照しながら説明する。ユーザはローカルネットワーク１側にＲＡＳ接続しようとするときに、クライアント装置３にインストールされている専用アプリケーションソフトウエアを起動する。まず、図３に示すようにクライアント装置３の制御部３１は、専用アプリケーションソフトウエアに従って、ユーザに対してユーザ名とパスワードとを入力するよう表示部３４に表示する（Ｓ１）。ユーザが操作部３５を操作して、第２認証情報（本発明の第１接続認証情報にも対応する）としてのユーザ名とパスワードとを入力すると（Ｓ２）、第１認証情報としての固有情報を演算して生成し（Ｓ３）、第１情報を生成した固有情報で復号し、第２情報を当該入力されたユーザ名で復号する。そしてこれらの復号結果が互いに一致するか否かを調べ（Ｓ４）、一致したときに、処理Ｓ２で入力されたユーザ名及びパスワードを第１の暗号化方法で暗号化する（Ｓ５）。この第１の暗号化方法で暗号化されたユーザ名及びパスワードが本発明の第２接続認証情報に対応する。またこのとき、定義情報に、暗号化パスワードの少なくとも一部が含まれる場合は、処理Ｓ５で暗号化したパスワードのうち対応する少なくとも一部と、定義情報に含まれている上記暗号化パスワードの少なくとも一部とが一致するか否かを比較し、一致しない場合は処理を中断してもよい。なお、暗号化したパスワードの全体で比較しないことにより、セキュリティがさらに向上する。
【００４２】
また制御部３１は、認証サーバ４のネットワークアドレスを復号し（Ｓ６）、復号して得たネットワークアドレスに対して、処理Ｓ５にて第１の暗号化方法で暗号化した第１暗号化ユーザ名及び第１暗号化パスワードとともに、接続要求を送信する（Ｓ７）。なお、処理Ｓ４において一致しなかった場合は、その時点で認証処理を中断する。
【００４３】
本実施の形態において特徴的なことの一つは、専用アプリケーションソフトウエアの処理として、処理Ｓ３に示すように、ＲＡＳ接続をしようとするごとに毎回、第１認証情報としての固有情報の演算を改めて行うことである。これにより他の認証情報が漏洩したとしても、一般に異なるコンピュータを用いた場合は異なる第１認証情報が演算される結果となるため、ＲＡＳ接続の処理が中断される。
【００４４】

認証サーバ４は、クライアント装置３から接続要求とともに受信した、暗号化されたユーザ名及びパスワードを受信し、記憶部４２を参照して、当該暗号化されたユーザ名及びパスワードを検索する（Ｓ１１）。ここで、当該暗号化されたユーザ名及びパスワードが記憶部４２に格納されていた場合は、当該暗号化されたユーザ名及びパスワードに関連付けられている、接続サーバ１１のネットワークアドレスを取得する（Ｓ１２）。なお、処理Ｓ１１にて当該暗号化されたユーザ名及びパスワードが記憶部４２に格納されていなかった場合（これらによる認証に失敗した場合）は、認証サーバ４は処理Ｓ１２以降の処理を行うことなく、処理を終了する。

【００４５】

また、認証サーバ４は、接続要求元のクライアント装置３のネットワークアドレス（クライアントアドレス）を取得する（Ｓ１３）。認証サーバ４は、処理Ｓ１２で取得した接続サーバ１１のネットワークアドレスに対して、処理Ｓ１３で取得したクライアントアドレスを送信して（Ｓ１４）、接続サーバ１１から接続待機状態に移行した旨を表す情報を受信するまで待機する（Ｓ１５）。このフローの続きは、図示の都合上、図４に示されている。

【００４６】

図４に上記フローの続きを示すように、接続サーバ１１は、認証サーバ４からクライアントアドレスを受信すると、当該ネットワークアドレスからのアクセスを、予め定められた一定の期間だけ受入可能に設定する（Ｓ２１）。この認証サーバ４と接続サーバ１１との間の通信は、専用回線や暗号化通信回線など、セキュアな回線を用いて行われることとしてもよい。具体的にクライアント装置３とのＲＡＳ接続を、ｐｐｔｐ（Point-to-Point Tunneling Protocol）を用いて行う場合、接続サーバ１１にファイアウオールを設定しておき、認証サーバ４からクライアント装置３のネットワークアドレスを受信したときに、ｐｐｔｐのポート（ＴＣＰのポート）を一定の期間（例えば６０秒）だけオープンする。そして、接続サーバ１１は、接続待機状態に移行した旨を認証サーバ４に対して送信する（Ｓ２２）。

【００４７】

認証サーバ４は、接続サーバ１１から接続待機状態に移行した旨を表す情報を受信すると、クライアント装置３に対して接続の指示を送信する（Ｓ３１）。クライアント装置３は接続の指示を受信すると、第２認証情報としてのユーザ名とパスワードとを第２の暗号化方法で暗号化して（Ｓ４１）、この第２の暗号化方法で暗号化した第２暗号化ユーザ名と第２暗号化パスワードとをｐｐｔｐにおけるユーザ名及びパスワードとして接続サーバ１１に送信する（Ｓ４２）。

【００４８】

ここで、処理Ｓ３１の接続の指示には、接続サーバ１１のネットワークアドレスを含めてもよい。この場合、接続サーバ１１のネットワークアドレスを、クライアント装置３に事前に設定しておく必要がない。また、この場合クライアント装置３は、処理Ｓ４２において、受信した接続の指示に含まれるネットワークアドレスで特定される接続サーバ１１に、第２の暗号化方法で暗号化した第２暗号化ユーザ名と第２暗号化パスワードとを送信することになる。これにより、クライアント装置のユーザは、認証用サーバにおいて認証を受けるまでは、接続サーバのネットワークアドレスを知ることもできないこととなり、セキュリティを向上できる。

【００４９】

なお、ここでは接続サーバ１１が接続待機状態に移行した旨を認証サーバ４に対して送信することとしているが、この送信は必ずしも必要ではない。この送信が行われない場合は、認証サーバ４は接続サーバ１１に対してクライアントアドレスを送信し、クライアント装置３に対して接続の指示を送信する処理（処理Ｓ３１）を行う。

【００５０】

接続サーバ１１は、この暗号化されたユーザ名とパスワードとが、登録されているユーザ名とパスワードに一致しているか否かを調べ（Ｓ５１）、一致している場合は、ｐｐｔ

ｐによる通信を開始する（Ｓ５２）。また、処理Ｓ５１において一致していない場合は、認証処理を中断する。ここでの第２の暗号化方法による暗号化も、必ずしも復号可能である必要はなく、例えばユーザ名のハッシュ値とパスワードのハッシュ値としてもよい（すなわち第１の暗号化方法と同じ方法であってもよい）し、所定の情報（例えば固有情報など、接続要求のたびごとに生成される情報や、接続サーバ１１側から取得されるチャレンジ情報（接続要求のたびに生成されるランダム値を含む情報））をユーザ名やパスワードをキーとしてそれぞれ暗号化したものであってもよい。

【００５１】

接続サーバ１１側では、ユーザ名等がＭＤ５などのハッシュ値として暗号化される場合は、登録されたユーザ名等のハッシュ値と比較することにより、一致するか否かを調べてユーザ名等の認証を行う。また、ユーザ名等をキーとして固有情報が暗号化されている場合は、登録されているユーザ名等と固有情報とを用いて同じように暗号化を行い、第２暗号化ユーザ名等を生成して、当該生成したものが受信したものと一致するか否かを調べてユーザ名等の認証を行う。

【００５２】

さらに、チャレンジ情報を用いる場合は、ランダム情報を含むチャレンジ情報を発行し、クライアント装置３側に当該発行したチャレンジ情報を提供し、ユーザ名等をキーとして暗号化されたチャレンジ情報を受信し、登録されているユーザ名等と発行したチャレンジ情報とを用いて同じように暗号化を行い、第２暗号化ユーザ名等を生成して、当該生成したものが受信したものと一致するか否かを調べてユーザ名等の認証を行う。

【００５３】

［接続処理］

このようにして認証が行われるため、たとえ途中で暗号化されたユーザ名やパスワードが漏洩したとしても、元のユーザ名を知ることは困難であるので、専用アプリケーションソフトウエアを操作することができない。また接続サーバ１１のポートをオープンさせるためには、認証サーバ４に対する攻撃が不可欠であり、接続サーバ１１に対する攻撃の頻度を低下させるうえ、基本的な認証が認証サーバ４にてまず行われることで、接続サーバ１１の処理負荷の軽減にも資している。さらに、仮にポートをオープンさせ、パスワード等の大量送信によるハッキングが可能となったとしても、ポートがオープンしている６０秒以内に、ユーザ名とパスワードとを調べあげる必要があるなど、事実上不正アクセスはできない。さらに、接続処理が完了したときには、当該接続に用いられたポートを閉じるようにしてもよい。また、接続サーバ１１のポートがオープンしている状態で、パスワードなどによる認証にあらかじめ定めた回数（例えば１回としてもよい）だけ失敗するとポートを閉じるようにしてもよい。

【００５４】

本実施の形態において、さらに特徴的なことの一つは、接続要求のたびに生成される情報を利用して、ユーザ名やパスワードの暗号化が行われるにもかかわらず、当該暗号化されたユーザ名によってユーザを特定できることである。従ってローカルネットワーク側では、ユーザごとにアクセス権を設定するなど、ユーザごとに対応した処理が可能となる。

【００５５】

また、接続サーバ１１は、ユーザごとに最終アクセス日時などのアクセス記録を生成し、記憶部１６に格納しておいてもよい。この場合、ユーザからアクセスが行われるごとに、当該ユーザに対して、当該ユーザが前回アクセスした日時の情報を記憶部１６から検索して提供する。これにより各利用者は、万が一、不正アクセスがあった場合でも、その事実を認識でき、セキュリティがより向上する。

【００５６】

またこのように、ユーザを特定できるので、ユーザごとに期限を設定することとしても好ましい。具体的には、接続サーバ１１はユーザごとに期限の情報を関連付けて保持しており、ｐｐｔｐによる通信を開始する前に、処理Ｓ５１にて認証したユーザの期限の情報と、図示しないカレンダの情報とを参照し、期限が到来しているか否かを調べ、到来して

いれば認証処理を中断して、接続を拒否し、到来していない場合は処理Ｓ５２に移行してｐｐｔｐによる通信を開始する。この期限の情報は、接続サーバ１１の管理者が更新して登録できるようにしておいてもよい。

【００５７】

なお、ここまでの説明では、クライアント装置３は、処理Ｓ５からＳ７により、第１暗号化ユーザ名及び第１暗号化パスワードとともに、接続要求を送信するようにしているが、まず第１暗号化ユーザ名とともに接続要求を送信し、認証サーバ４がこの接続要求を受けて発行したチャレンジ情報（ランダム情報を含む）を受信して、当該チャレンジ情報を第１暗号化パスワードをキーとして暗号化して送信するなど、パスワードについては、いわゆるチャレンジレスポンスを利用した認証を行ってもよい。

【００５８】

このことは、接続サーバ１１との間でも同様であり、ここまでの説明では第２の暗号化方法で暗号化した第２暗号化ユーザ名と、第２暗号化パスワードとを生成して接続サーバ１１に対して送信していたが、パスワードについては、第２の暗号化方法による暗号化をすることなく、一部のｐｐｔｐにおいて実装されている、チャレンジレスポンスを利用した認証を行うようにしてもよい。

【００５９】

また、接続サーバ１１の第１通信制御部１７のネットワークアドレスは、固定的に設定されていても、時間とともに変化してもよい。すなわち、ここでいうネットワークアドレスがＩＰアドレスである場合、スタティックであっても、ダイナミックであっても構わない。接続サーバ１１は、自己の第１通信制御部１７に割り当てられるネットワークアドレスが変更されたときには、変更後のネットワークアドレスを認証サーバ４に対して送信してその登録を更新させる。

【００６０】

さらに、ここでは、クライアント装置３とのＲＡＳ接続の通信プロトコルとしてｐｐｔｐを用いる例について述べたが、これに限らず、ＩＰＳＥＣやＶＰＮ－ＨＴＴＰＳ等、他のセキュアな通信プロトコルを用いても構わない。

【図面の簡単な説明】

【００６１】

【図１】本発明の実施の形態に係るネットワーク接続システムの例を表す構成ブロック図である。

【図２】認証サーバ内に格納されているデータの一例を表す説明図である。

【図３】本発明の実施の形態に係るネットワーク接続の前半部分の流れの例を表すフロー図である。

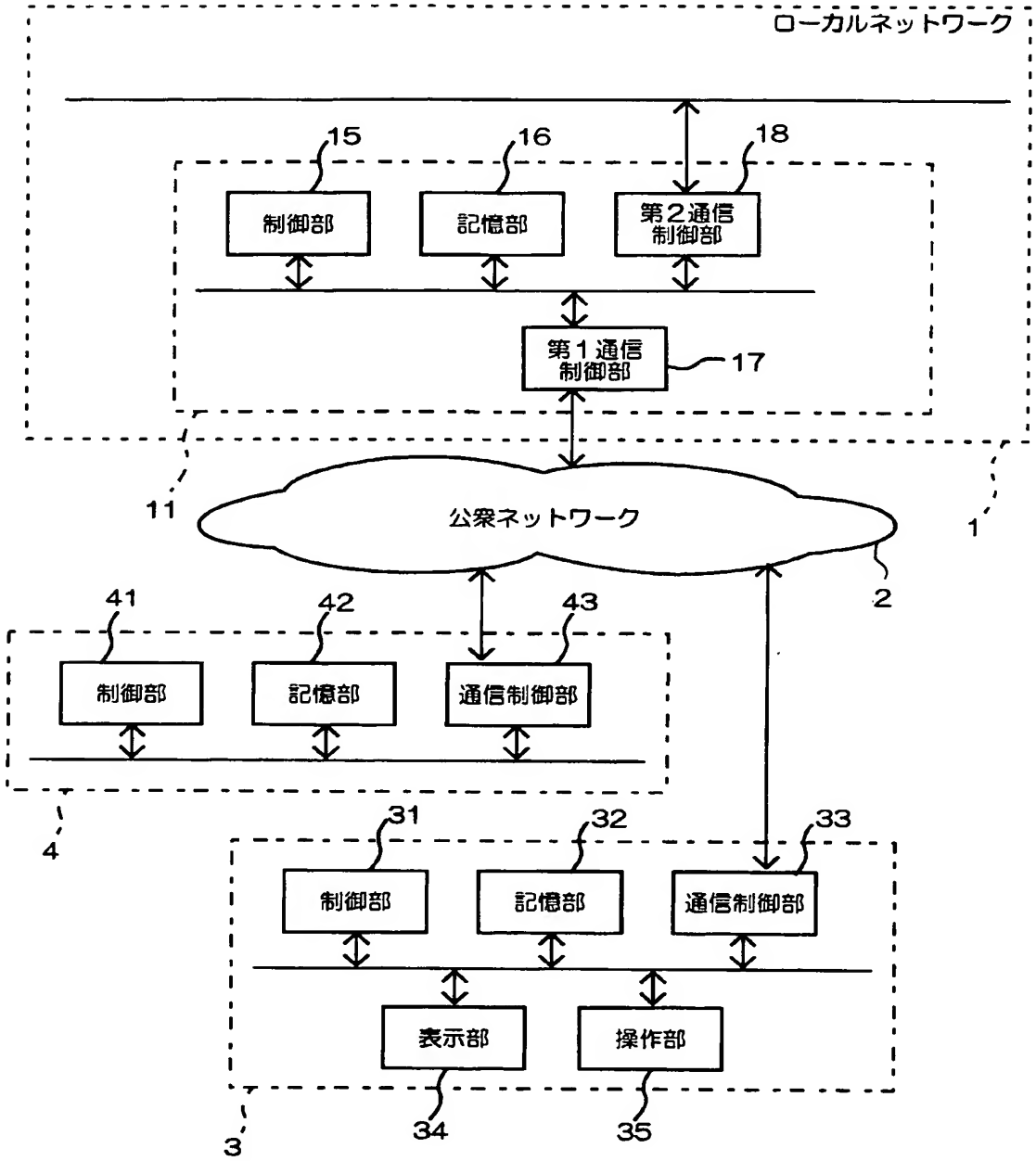
【図４】本発明の実施の形態に係るネットワーク接続の後半部分の流れの例を表すフロー図である。

【符号の説明】

【００６２】

１　ローカルネットワーク、２　公衆ネットワーク、３　クライアント装置、４　認証サーバ、１１　接続サーバ、１５，３１，４１　制御部、１６，３２，４２　記憶部、１７　第１通信制御部、１８　第２通信制御部、３３，４３　通信制御部、３４　表示部、３５　操作部。

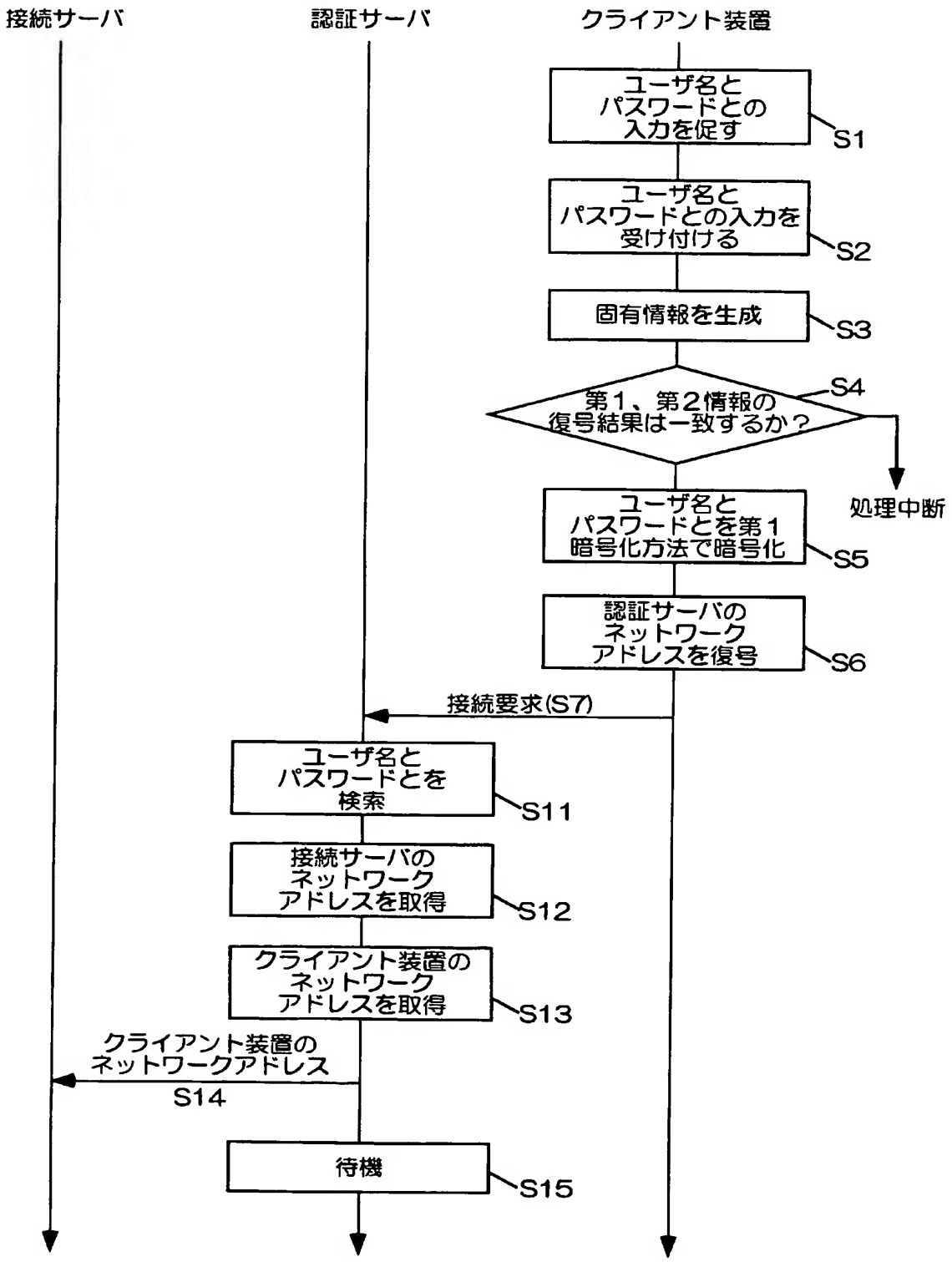
【書類名】図面
【図１】


ローカルネットワーク
15
16
18
制御部
記憶部
第２通信制御部
第１通信制御部
17
11
公衆ネットワーク
1
2
41
42
43
制御部
記憶部
通信制御部
4
31
32
33
制御部
記憶部
通信制御部
表示部
操作部
34
35
3

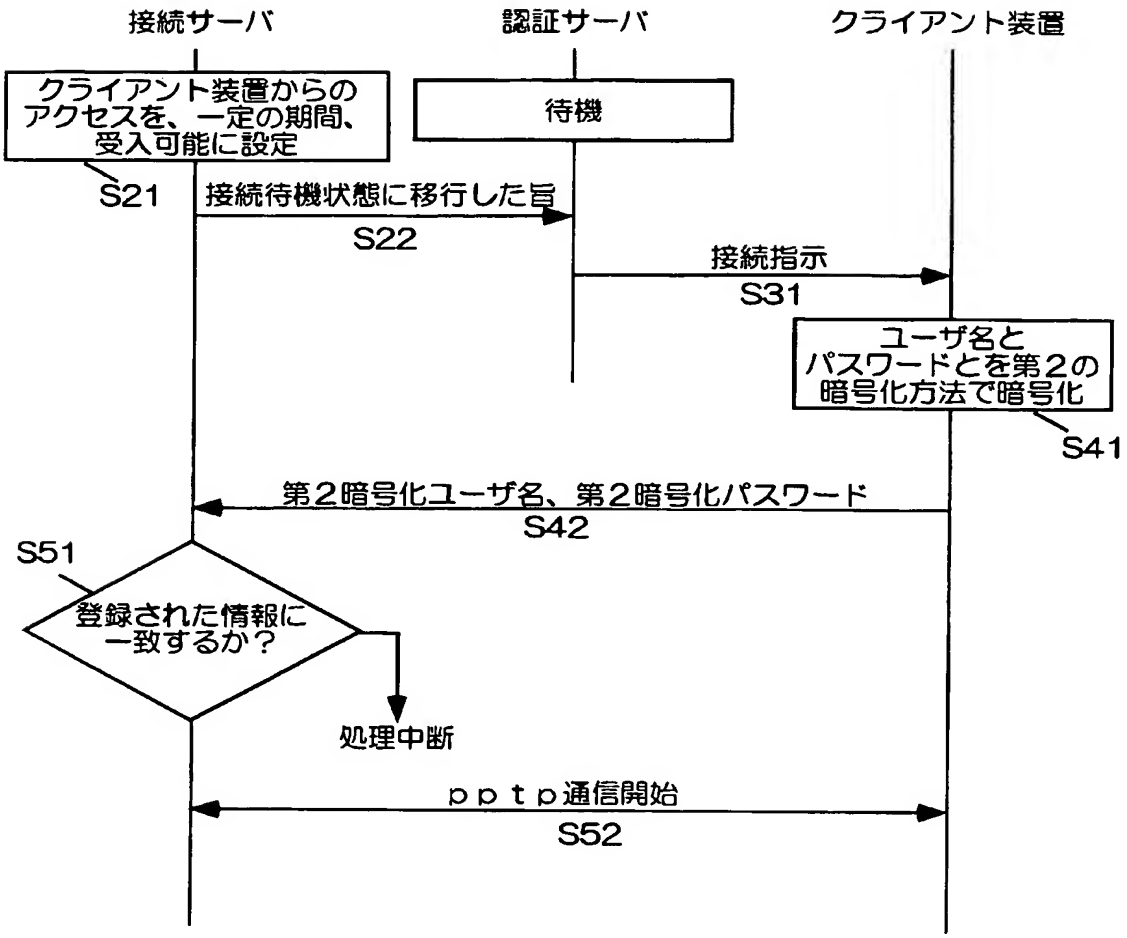
【図２】

接続サーバの ネットワークアドレス	第１暗号化 ユーザ名	第１暗号化 パスワード
aaaaa	bbbb	ccccc
aaaaa	ddddd	eeeee
fffff	ggggg	hhhhh
aaaaa	xxxxx	yyyyy
⋮	⋮	⋮

【図３】


接続サーバ
認証サーバ
クライアント装置
ユーザ名と
パスワードとの
入力を促す
S1
ユーザ名と
パスワードとの入力を
受け付ける
S2
固有情報を生成
S3
第１、第２情報の
復号結果は一致するか？
S4
処理中断
ユーザ名と
パスワードとを第１
暗号化方法で暗号化
S5
認証サーバの
ネットワーク
アドレスを復号
S6
接続要求(S7)
ユーザ名と
パスワードとを
検索
S11
接続サーバの
ネットワーク
アドレスを取得
S12
クライアント装置の
ネットワーク
アドレスを取得
S13
クライアント装置の
ネットワークアドレス
S14
待機
S15

【図４】


接続サーバ
認証サーバ
クライアント装置
クライアント装置からのアクセスを、一定の期間、受入可能に設定
S21
待機
接続待機状態に移行した旨
S22
接続指示
S31
ユーザ名とパスワードとを第２の暗号化方法で暗号化
S41
第２暗号化ユーザ名、第２暗号化パスワード
S42
S51
登録された情報に一致するか？
処理中断
ｐｐｔｐ通信開始
S52

【書類名】要約書
【要約】
【課題】　リモートアクセスにおけるセキュリティを向上できるネットワーク接続システムを提供する。
【解決手段】　クライアント装置３と、認証用サーバ４と、接続サーバ１１とを含むネットワーク接続システムであって、認証用サーバ４がクライアント装置３のユーザを認証し、接続サーバ１１にクライアント装置３のネットワークアドレスを通知する。接続サーバ１１から接続待機状態に移行した旨を表す情報を受信すると、当該ネットワークアドレスをクライアント装置３に対して送出し、クライアント装置３が当該ネットワークアドレスに暗号化したユーザ名とパスワードとを送信して、接続サーバ１１が、当該暗号化されたユーザ名及びパスワードを用いた認証を行う。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００４－０３５４８１
受付番号	５０４００２２７２３６
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１６年　２月１７日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000005496
【住所又は居所】	東京都港区赤坂二丁目１７番２２号
【氏名又は名称】	富士ゼロックス株式会社

【代理人】　申請人

【識別番号】	110000154
【住所又は居所】	東京都新宿区新宿二丁目４番１６号　栄幸ビル９階
【氏名又は名称】	特許業務法人はるか国際特許事務所

特願２００４－０３５４８１

出　願　人　履　歴　情　報

識別番号　［０００００５４９６］

１．変更年月日　１９９６年　５月２９日
［変更理由］　住所変更
住　所　東京都港区赤坂二丁目１７番２２号
氏　名　富士ゼロックス株式会社